Microsoft Defender for Cloud

@chadmcrowell.com
/in/chadmcrowell
kubeskills.com

CYBR

Network Security

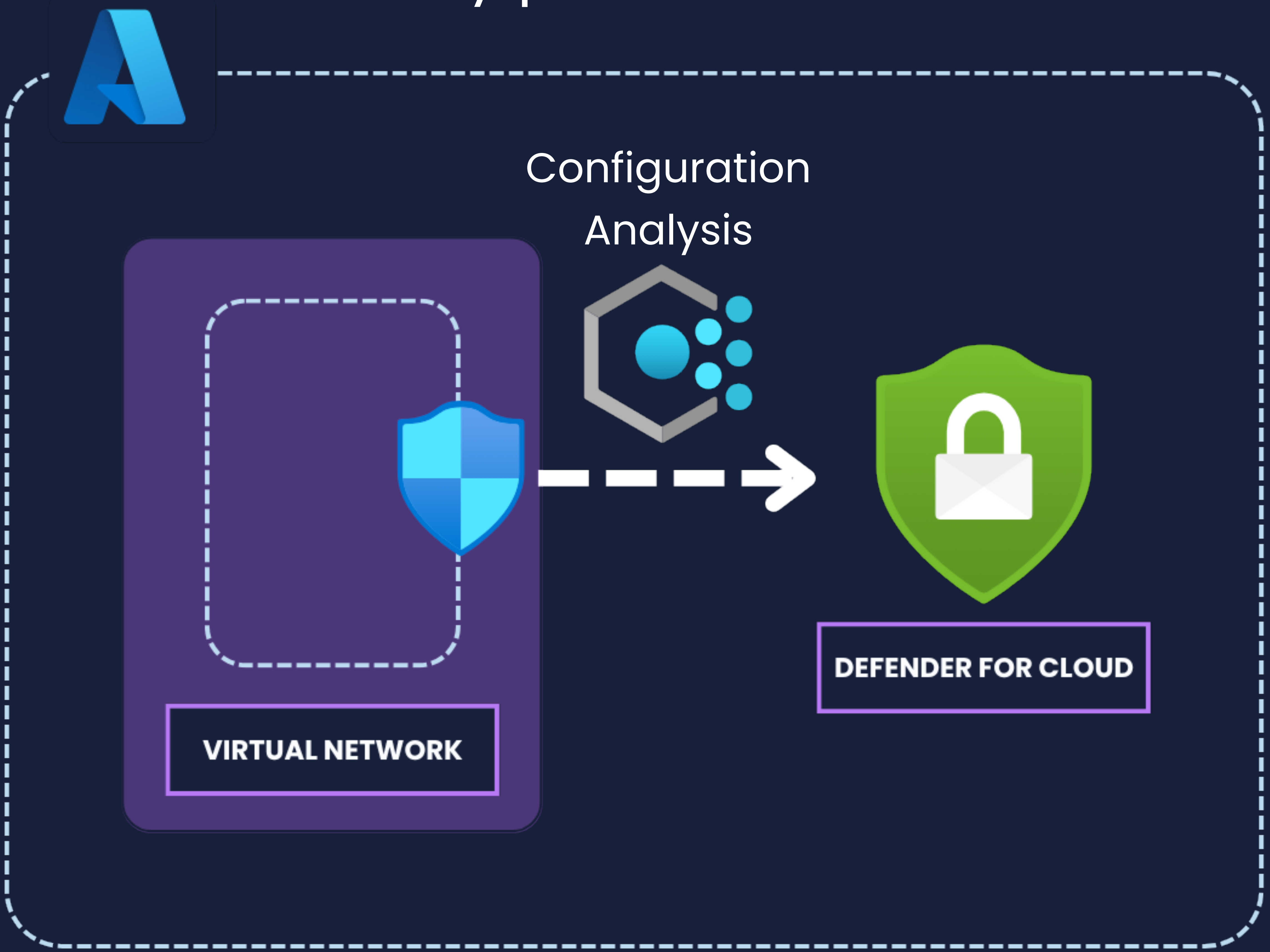
Microsoft Defender for Cloud

@chadmcrowell.com
/in/chadmcrowell
kubeskills.com

CYBR

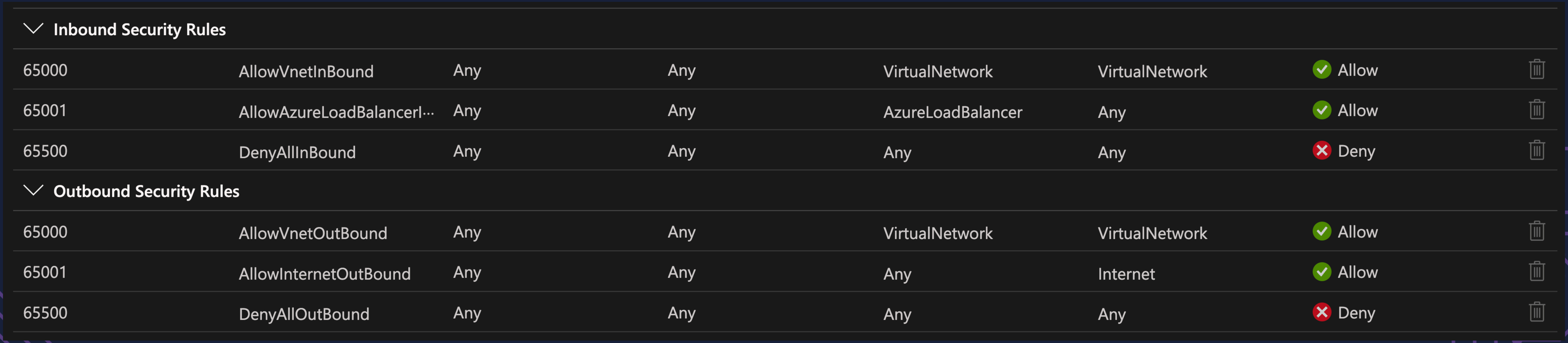
Defender for Networking (NSGs)

Monitoring and analyzing Network Security Groups (NSGs) and their rules to detect overly permissive access and exposed ports



Network Security Groups (NSGs)

- Source & destination IP ranges
- Port ranges
- Protocols (TCP/UDP)
- Priority (lower number = higher priority)
- Action (allow or deny)



Inbound Security Rules						
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerI…	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	✓ Allow
65500	DenyAllOutBound	Any	Any	Any	Any	✗ Deny

Flow Logs

- NSG flow logs deprecated
- **NEW** VNET Flow Logs
- Analyze actual traffic for deep insights
- Anomaly detection or diagnostics
- Integrating with Sentinel or Azure Monitor

https://learn.microsoft.com/en-us/azure/network-watcher/vnet-flow-logs-overview

Microsoft Defender for Cloud

@chadmcrowell.com
/in/chadmcrowell
kubeskills.com

CYBR

THANK YOU!